Note d'information

Permettre un Accès en Toute Sécurité aux Espaces Numériques

Introduction

Le programme d'inclusion numérique du HCR reconnaît le droit des réfugiés et d'autres populations contraintes de fuir à participer activement à la révolution numérique actuelle. Les contextes humanitaires face à la pandémie COVID-19 ont souligné l'importance cruciale d'une communauté de réfugiés connectée qui peut accéder efficacement à distance à des informations vitales et à des services de protection vitaux.

Toutefois, outre ces possibilités, faciliter l'accès numérique et l'inclusion des personnes déplacées de force et de leurs communautés d'accueil peut, par inadvertance, entraîner des risques pour les individus. Qu'il s'agisse de cas de fraude en ligne, d'utilisation abusive des données des réfugiés qui sont saisies au moment où ils se connectent ou de traçage des activités sur les médias sociaux, ces risques doivent être compris, gérés et atténués dans la mesure du possible. En outre, il est primordial que les personnes relevant de la compétence du HCR disposent des compétences et des systèmes adéquats pour s'engager en toute sécurité sur Internet afin de pouvoir utiliser en toute confiance les outils numériques disponibles pour accroître leur résilience. En lien avec les récents travaux du ICRC (International Committee of the Red Cross) explorant les risques de protection des données dans les interventions de connectivité, le HCR souhaite mieux comprendre comment ces risques se manifestent et quelles actions peuvent être prises pour minimiser les risques auxquels les communautés sont confrontées du fait de leur accès numérique. Une première exploration du sujet a été entreprise dans Connecting With Confidence: Managing Digital Risk rapport suivant qui décrit plus en détail certaines des problématiques sur ce sujet et met en évidence l'expérience des personnes relevant de la compétence du HCR dans deux pays (Ouganda et Kenya).

Contexte

La culture numérique est essentielle pour que les individus puissent utiliser la technologie de manière sûre, efficace et effective. Le manque de compétences et de connaissances numériques reste un des principaux obstacles à l'accès aux services de connectivité dans le monde entier. À une époque où les sociétés dans leur ensemble se numérisent rapidement et où l'aide humanitaire est de plus en plus fournie par des réseaux et outils numériques, il est essentiel de combler ce déficit de compétences pour que les communautés soient en mesure de maîtriser les outils numériques souvent nouveaux et peu familiers. En outre, la maîtrise des données numériques est également très importante car les membres de la communauté doivent pouvoir non seulement maîtriser les outils et les plateformes qu'ils utilisent, mais aussi ce qu' advient des données qu'ils produisent ou fournissent, comment elles sont traitées et par qui. Il existe également différentes manières de relever ces défis, allant de campagnes d'information à des approches menées par les communautés elle-même pour améliorer leur compréhension.

Cependant , les risques ne s'arrêtent pas à la maîtrise des outils numériques et des données par les populations. D'autres risques possibles existent, tels que:

1. **Connexions Sécurisées:** La majorité de la connectivité à laquelle ont accès les réfugiés ou les personnes déplacées est fournie par des connexions cellulaires opérées par des opérateurs de réseaux mobiles. Dans certains contextes, cependant, la connectivité est assurée par des points d'accès WiFi, des centres communautaires connectés et d'autres solutions locales. La nature spécifique de ces connexions peut entraîner des risques : Un filtrage du contenu est-il en place? Combien de temps les données sont-elles conservées lorsque les réfugiés utilisent les points d'accès? Ces réseaux locaux sont-ils sûrs ou vulnérables aux attaques? Comment ces centres sont-ils opérés et par qui? Des mesures simples peuvent être prises pour gérer les risques de sécurité de l'infrastructure des réseaux locaux;
2. **Surveillance Numérique:** Comment les informations personnelles sont-elles utilisées en ligne - consciemment ou inconsciemment? Comment d'autres partis peuvent-ils surveiller, enregistrer et utiliser l'empreinte numérique et le comportement en ligne d'une population? Dans quelle mesure les personnes relevant de la compétence du HCR sont-elles conscientes de ce problème et comment cela pourrait les affecter à l'avenir lorsqu'elles cherchent de l'aide ou des solutions?
3. **Sécuriser l'Accès:** Les comptes en ligne et les dispositifs personnels contiennent des informations personnelles précieuses mais souvent celles-ci ne sont pas protégées de manière adéquate, par exemple des mots de passe ou des informations sur les comptes sont partagés sans nécessairement comprendre les risques. Il est essentiel de comprendre comment gérer les mots de passe, les paramètres de sécurité et de confidentialité, et les implications plus larges du partage des données d'accès pour les connexions ou les services afin de réduire au minimum le risque d'accès illégitime;
4. **Cybercriminalité:** Elle peut prendre diverses formes, comme l'usurpation d'identité en ligne, la fraude financière, le harcèlement, l'intimidation, le piratage, l'usurpation de courrier électronique, le piratage et la falsification d'informations et la propriété intellectuelle;
5. **Les abus en ligne et la violence sexuelle:** Les médias sociaux tels que Facebook et Instagram ont été utilisés pour faciliter la traite des êtres humains et l'exploitation sexuelle (par exemple, en se mettant en contact avec des victimes potentielles par le biais de fausses offres d'emploi ou en se liant d'amitié avec des enfants). En outre, l'utilisation généralisée de la technologie numérique a entraîné une augmentation du harcèlement en ligne ou des interactions sexuelles non sollicitées, touchant particulièrement les femmes et les jeunes filles.

Portée et objectifs

L'objectif principal de ce défi est de s'appuyer sur les efforts précédents des organisations humanitaires et des ses partenaires et de garantir un accès durable à la connectivité aux réfugiés et à leurs communautés d'accueil pour faire face aux risques numériques réels et perçus et garantir un engagement en ligne securisé, inclusif et responsable - en tenant compte des risques et obstacles spécifiques rencontrés par les différents groupes en fonction de l'âge, du sexe ou de la démographie.

Application

Les interventions proposées visent donc à répondre aux risques auxquels sont confrontées les communautés sur internet dans un contexte opérationnel donné en améliorant leurs compétences numériques. Les interventions peuvent:

1. Sensibiliser aux risques sur internet ,réels et perçus, y compris les risques les plus pertinents et les groupes spécifiques ciblés parmi les réfugiés et autres populations vulnérables, dans des formats accessibles;
2. Fournir les outils nécessaires à un engagement plus sûr en ligne, en protégeant l'identité des personnes, en identifiant les informations clés à protéger et en partageant les données personnelles de manière responsable;
3. Établir des protocoles pour le personnel, les partenaires et les personnes relevant de la compétence du HCR afin de pouvoir détecter les menaces en ligne éventuelles et de comprendre comment y répondre efficacement ou les signaler de manière appropriée.

Pour soumettre une manifestation d'intérêt à ce défi, cliquez sur le bouton Appliquer Maintenant.

APPLIQUER MAINTENANT

(*Vous devrez vous connecter à votre compte HCR*)